The European Union's *General Data Protection Regulation* and Collaborative Driving: Riding On the Edge of Lawfulness?

MAURICE SCHELLEKENS*

Abstract

This article focuses on a system that can warn the driver of a car of dangerous driving situations. This system relies on V2V communication: each vehicle communicates data concerning its position, heading, and speed to surrounding vehicles and does so with a high frequency. Sharing of precise location data with a high frequency raises data protection questions. Although technical measures are taken to shield the identity of drivers, risks of identification remain substantial. In light of these circumstances, is it possible to process location data in a lawful way as required by article 5 of the European Union's data protection law, the General Data Protection Regulation *('GDPR')*[1]*? This article examines whether the processing of location data can be brought under one of the lawful grounds for processing listed in article 6 of the GDPR. In doing so, this article contributes to the discussion of whether the GDPR is fit for purpose in modern horizontal applications.*

1 *Introduction*

There is much publicity about self-driving cars. Predictions are made that they will soon enter our roads. Reality is that it is quite challenging to make a self-driving car behave adequately in all situations that can be encountered on the road. Another road traffic innovation that is much closer to implementation is often overlooked, even though it has profound implications just the same. This innovation is vehicle-to-vehicle ('V2V') communication, vehicle-to-infrastructure ('V2I') communication, and vehicle-to-everything ('V2X') communication. With these innovations, vehicles will communicate with each other, with the road infrastructure, and with other devices, such as body-worn devices of pedestrians. These communications allow for collaborative driving, among other things.

[*] The author is Senior Researcher at Tilburg University, Tilburg Institute for Law, Technology, and Society, Tilburg, Netherlands. This article reflects the law and technological environment as at the time it passed double-blind peer review in 2020.

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 *('GDPR').*

Collaborative driving belongs to the domain of Cooperative Intelligent Transport Systems ('C-ITS') and it brings advantages in safety (advance warnings of danger), traffic flow (reduction of traffic jams), and environmental protection (less pollution). However, beyond collaborative driving, V2-Communication also has other applications. For example, cars will become mobile commerce ('m-commerce') platforms. Initial applications in that domain may include the downloading of content, such as movies that rear-seat passengers can watch on their screens.

This article concentrates on an early application of C-ITS: a safety warning system. Through V2V and V2I communications, vehicles can warn their human drivers for dangers that the drivers themselves cannot detect and that even an on-board radar may not be able to detect (for example, where there is no line of sight to the source of danger). In different world regions, different consortia are developing the technology. In Europe, the Car-to-Car Communication Consortium ('C2C Consortium') is the forerunner in this field. It includes major manufacturers such as BMW, Daimler, Ford, Honda, Renault, Toyota, Volkswagen, and Volvo.[2]

The technology requires that vehicles communicate intensely with each other and very regularly make their location known to other vehicles in their vicinity. Since vehicles are closely related to persons (their owner, driver, and passengers if there are any), such communication touches upon privacy and data protection issues. In theory and perhaps also in practice, it opens up new possibilities to track or trace persons. Even though location information is sensitive from a data protection perspective, one may question whether this creates new problems in data protection. After all, almost everybody already carries a mobile smartphone with GPS capability. Nonetheless, the safety warning system and its underlying V2V capabilities have characteristics that set it apart from cell phones. One of the main remarkable features is the horizontal, peer-to-peer like setup of the system.

Under article 5 of the European Union's data protection framework, the *General Data Protection Regulation* ('GDPR'), personal data must be processed lawfully, among other requirements. Article 6 of the Regulation provides that processing will only be lawful if at least one of the grounds listed in that provision apply. Given the potential data protection implications of this system, it is unclear whether a lawful basis for the processing of location information involved in the safety application can be found under article 6. This article examines whether there is such an applicable ground and, if there is, which one.

This article proceeds as follows. Section 2 explains how the safety warning system is set up and elaborates on the risks that data subjects are exposed to. It pays special attention to technical measures that are taken to reduce concerns about

[2] For the full list, see 'Partners of the CAR 2 CAR Communication Consortium', *Car 2 Car Communication Consortium* (Web Page) <https://www.car-2-car.org/membership/>.

privacy and data protection, namely privacy-by-design and privacy-by-default.[3] It should be noted, however, that the precise technical set-up of these measures is still under development.[4] Section 3 then turns to matters of privacy and data protection. Specifically, Section 3.1 examines whether the messages processed in a V2V safety warning system are personal data. Section 3.2 explores whether a ground under article 6 of the GDPR can be found to allow the lawful processing of personal location data in the context of the warning system.

2 *A V2V Safety Warning System*

V2V communication has many applications. As stated above, this article focuses on one of the first applications: a safety warning system. In this application, vehicles communicate their positions to each other. This information is used to give advance warnings to the drivers of the vehicles for dangerous situations, such as approaching stationary vehicles in the road or other vehicles braking hard. The interface of the safety application on the dashboard gives a warning to the driver of the car, alerting them to imminent dangers.

For this safety application, V2V communication has advantages over other technologies. If two cars approach a crossroad from different directions, and there is no line of sight to each other, safety technologies like radar are seriously hampered in providing a timely safety warning to motorists. In contrast, V2V communication uses 'radio waves' and therefore it is not affected by objects blocking a line of sight.

The choice between different radio technologies — Wi-Fi or 5G-based — has been heavily contested. The European Commission, the European Parliament and a faction of the automotive industry see WiFi-based technologies as the most promising solution, since it is mature enough for introduction on the road in the short term.[5] Meanwhile, the European Council and another faction of the

[3] The Commission is studying data protection by design and by default, specifically related to C-ITS: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy on Cooperative Intelligent Transport Systems, a Milestone Towards Cooperative, Connected and Automated Mobility' (COM(2016) 766 final, 30 November 2016) 8. See also C-ITS Platform, 'Final Report' (21 January 2016).

[4] *Annex to the Commission Decision of 11 December 2018 updating the Working Programme Related to the Actions Under Article 6(3) of Directive 2010/40/EU [2018] C(2018) 8264 final, 3.*

[5] *Commission Delegated Regulation (EU) …/... Of 13 March 2019 Supplementing Directive 2010/40/EU of the European Parliament and of the Council with Regard to the Deployment and Operational Use of Cooperative Intelligent Transport Systems* [2019] C(2019) 1789 final; Agence Europe, *European Parliament Gives Green Light to Delegated Act on Deployment of Cooperative Intelligent Transport Systems, Europe Daily Bulletin No 12238* (Article, 18 April 2019) <https://agenceurope.eu/en/bulletin/article/12238/6>.

automotive industry favour 5G, even though it may delay introduction of a safety warning system.[6] This article takes Wi-Fi based solutions as a starting point since this option was elaborated further at the time of writing, thus facilitating the data protection analysis.

Regarding Wi-Fi technologies, the Institute of Electrical and Electronics Engineers ('IEEE') is developing a family of standards that lay down technical specifications for V2V Wifi. These are the 1609 802.11p standards. This is a modification of the normal WiFi technology and there is a frequency band reserved for V2V communications. The deployment of 802.11p WiFi has been considered in both the United States ('US') and the European Union ('EU'). However, when it comes to the higher layers in the protocol stack, there are important differences between the European and US approaches.

The US chooses an 'awareness-based approach'. Each vehicle broadcasts its location data multiple times per second. All vehicles that are within range receive its messages. It is up to the *receiving* vehicle to sort out the location data received from all the cars in the vicinity and determine whether there is a risk of an accident that the driver needs to be warned about.

Meanwhile, the EU chooses an 'event-based approach'. If a car is involved in an event (it brakes hard, breaks down, approaches crossroads), it broadcasts a safety message. Hence, in the event-based approach, the *sending* vehicle interprets whether there is a danger and it only sends messages when there is. Its broadcast is limited to the geographic direction from which traffic can be expected for which the safety message is relevant. Cars receiving the safety message will forward this message to traffic further down the road. A drawback of an event-based system is that it can only warn for known (ie predefined) events. However, much fewer messages are needed than in an awareness-based system. Hence, there is much less risk of message traffic congestion.

In the EU, CAM7 and DENM8 are European standards detailing the contents of safety messages. In the US, the contents of safety messages are governed by the

[6] Agence Europe, *EU Council Confirms Objection to Delegated Act on Deployment of Cooperative Intelligent Transport Systems, Europe Daily Bulletin No 12291* (Article, 9 July 2019) <https://agenceurope.eu/en/bulletin/article/12291/30>.

[7] European Telecommunications Standards Institute, *ETSI EN 302 637-2 V1.3.2 (2014-11), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service* (European Technical Standard, 2014)

[8] European Telecommunications Standards Institute, *ETSI EN 302 637-3 V1.2.2 (2014-11), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralised Environmental Notification Basic Service* (European Technical Standard, 2014).

BSM9 standard. In both systems, precise location information of the sending vehicle is included in the message-content.

Table 1 summarises the most important characteristics of the two systems.[10]

Table 1: Characteristics of V2V Safety Warning Systems in the US and the EU

	US	**EU**
Warning functionality	Awareness-based	Event-based
Standards for safety message contents	Basic Safety Message ('BSM')	Cooperative Awareness Message ('CAM'), Decentralised Environmental Notification Message ('DENM')
Transport layer	WAVE Short Message Protocol ('WSMP') for safety messages and TCP/UDP for non-time critical location-based services	
Routing/Network Layer (OSI Protocol Stack)	WSMP for time-critical safety messages (**Single Hop Broadcast**) and IPv6 for non-time-critical LBS	GeoNetworking ('GN') for time-critical safety messages (**Multi Hop Geo Broadcast**) and IPv6 for non-time-critical LBS
Standards for Wireless Access in Vehicular Environment ('WAVE') or Direct Short Range Communication ('DSRC'). **MAC/Data Link Layer (OSI protocol Stack)**	IEEE 1609 802.11p family of standards (an adaptation of the 'normal' WiFi standards)	Direct Short Range Communication ('DSRC') based on IEEE 1609 802.11p (WiFi). Alternatives: LTE and 5G[11].

[9] SAE, *Dedicated Short Range Communications (DSRC) Message Set Dictionary, J2735 BSM* (Technical Standard, 19 November 2009).

[10] For an overview of the various initiatives relating to Vehicle Ad Hoc Networks ('VANETS'): Patrick I Offor, 'Vehicle Ad Hoc Network (VANET): Safety Benefits and Security Challenges' (2012) <https://ssrn.com/abstract=2206077>.

[11] Alessio Filippi et al, 'Why 802.11p Beats LTE And 5G For V2X', *EE News Automative* (online article, 21 April 2016) 8 <https://www.eenewsautomotive.com/design-center/why-80211p-beats-lte-and-5g-v2x>.

For manufacturers, the starting point is that 'the privacy' of motorists should be protected. Ideally motorists should remain unidentified. Therefore, the messages do not contain personal names, license plates, or Vehicle Identification Numbers ('VINs'). However, messages do contain technical identifiers such as a MAC-address or a public key (certificate). The contents of the messages contain data on the place, speed, and direction of the vehicle. The relevant question is: would somebody be able to link the technical identifiers or contents of a message to the identity of a driver or vehicle owner? In a system that communicates a car's position up to ten times a second to all cars and roadside units in its vicinity (ie less than 500 metres away, or at least in that order of magnitude), this possibility of identification is not inconceivable, as we will see below.

2.1 The Risk of Identification

How can the 'unidentified' state of a participating motorist come under threat? It is imaginable that a motorist is incidentally identified. For example, a mechanic performing maintenance on a car may be able to link a public key to an identity. Such incidental identification is generally not a big privacy threat because of the limited utility of incidental information. Therefore, this paper will concentrate on risks of large scale identification or identification that is possible in a systematic way. The largest risks in this respect are first, the large-scale collection and linking together of messages pertaining to a car and second, access to one or more central databases that contain directly identifying information, such as names of persons. The two categories of risks are elaborated below.

2.2 Systematic Collection of Messages

If somebody succeeded in collecting messages over a longer period of time and could tell which messages originate from the same car (for example, because a car uses messages with a persistent identifier), this may allow inference of a driver's identity. If you know where a car is parked overnight, where it is parked between 9:00h and 17:00h during working days, what its usual driving patterns are,[12] and so on, very little additional information is needed to arrive at the identity of the driver. This additional information need not be derived from physical observation. It may also derive from publicly available information sources, such telephone directories, SNS, census data etc. Research about location data generated by cellular telephony suggests that you typically need no more than 4 spatio-time points to arrive at a unique identification.[13] This means that

[12] If a car broadcasts a last message from a location before it is switched off and sometime later broadcasts a new message from the same location (after its engine has been started), then it is a safe inference that the car has been parked at that location between the two broadcasted moments. This holds for an awareness-based system. In an event-based system, parking will normally not trigger a message. If the same route is driven daily, this will eventually also show up in location data from an event-based system.

[13] Yves-Alexandre de Montjoye et al, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 *Scientific Reports* 1376; Yves-Alexandre de Montjoye et al

only one cellular phone was present at those four times in those exact four places. That does not yield the identity of the user: you may only know the IMSI or IMEI number. However, it does mean that additional information (from which you might derive an identity) needs to concern only those four spatio-time points.[14]

Who is in a position to theoretically be able to collect messages on a large scale in the C-ITS context? A number of likely candidates come to mind:

- Road managers with many roadside units.

- Providers of additional services on top of the basic safety warning service. For example, a traffic management service which, through roadside units, can receive messages in its central databases from cars indicating their locations. The service may use this information to see where the roads are busy and traffic jams are developing.

- Networked roadside services such as a chain of restaurants or fuelling stations. They can use their network of physical roadside facilities to receive messages and may have business interests in collecting these messages, such as for marketing purposes — what percentage of the road users actually makes use of their services?

- Fleet owners. They may use the cars in their fleet to collect messages, for example to generate their own traffic information to help other fleet drivers find less congested roads.

- Hackers. They may use botnet type of strategies: hacking into roadside units or even into cars to tap into the messages received by them.

- Individuals who collect messages of vehicles in their vicinity and share the data on the internet.

A privacy-friendly circumstance is that many 'reception networks' are not very fine-grained. A privacy-unfriendly circumstance is that the location of a vehicle is known with great precision (it is indicated in the contents of the message) and a reception point such as a fuelling station collects messages in a relatively wide area: Wi-Fi travels up to a kilometre. Hence, it is not just the vehicles passing by the fuelling station whose messages can be collected. Rather, those from cars on other nearby roads can also be collected.

'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347(6221) *Science* 536.

[14] Hui Zang & Jean Bolot, 'Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study', *Mobicom '11, Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, 145; Philippe Golle and Kurt Partridge, 'On the Anonymity of Home/Work Location Pairs' in Hideyuki Tokuda et al (eds), *Pervasive Computing (Lecture Notes in Computer Science #5538* (Springer, 2009).

2.3 Centralised Databases

An attractive route to finding an identity is a central database that already contains identities. What are examples of such central databases? If car manufacturers install the On-Board-Units ('OBUs') in cars, they may have databases linking OBU serial numbers to the VIN of the car in which it is installed. The sales organisation may have databases that link VINs to the names of customers who bought the cars. Another example of interesting databases are those held by Registration Authorities (who handles requests for digital certificates and registers them) and Certificate Authorities (who issue the certificates). Safety messaging obviously aims at increasing road safety. Hence, it is necessary that the messages sent come from reliable sources. So, OBUs need to authenticate themselves as 'official' and 'trustworthy' safety message generators. Public Key Infrastructure, based on verification digital certificates, is used to realise this. An OBU authenticates itself with one or more certificates. The certificates only prove that the OBU is authorised to participate in the safety warning system. It does not disclose an identity. However, if an OBU 'goes bad', its certificate (or certificates, if there are multiple) need to be revoked. Hence, inferences may be made about what certificates are being used by one and the same car. The central databases containing this information may be attractive targets for hackers.

Above, two different types of threats have been described, with a focus on how an identity of a motorist can be discovered. This is a precondition for possible further privacy invasions, such as surveillance of identified persons. Another problem is that once an identity is discovered based on a limited number of entries in a database with messages, all other stored messages about this car can easily be retrieved. From this, a historical picture of travels can be composed.

The linking pin between all threat types are the technical identifiers in messages. Given the threat types described above, the conclusion is that the use of technical identifiers in messages instead of identities (such as real world names, VINs, or license plates) only gives a superficial protection against identification. Therefore, the Car2Car Consortium has chosen to take further technical measures to prevent identification.

The core goal underlying the technical measures is to make it more difficult to derive an identity from technical identifiers. The strategy is to use technical identifiers in messages only temporarily and to change them regularly. The idea is that a temporary identifier does not yield enough information to derive an identity as described in the first threat type. An additional advantage is that, even if somebody succeeds in linking a technical identifier to a real-world or an otherwise usable identity, they may at best benefit from the identification only for a very short time. The implication of temporary usage is that all technical identifiers used in the protocol stack need to be changed regularly. These include the MAC-address and the public key certificate that authenticates the messages. In the realm of safety warnings, the TCP-IP stack is not used, so there is no IP address that needs to be 'rotated'. Location Based Services in the V2I realm do use the TCP-IP stack, but these are applications that go beyond the scope of this article and are therefore not dealt with here.

While the idea of temporary usage of identifiers is simple, its realisation is not so easy. Specifically, the design must prevent an attacker from observing an identifier change. If one identifier stops being used and another identifier pops up at the same time, an attacker may make an educated guess that they have witnessed an identifier change. In computer science literature, several solutions to this problem have been proposed and discussed,[15] including silent-periods, mix-zones, and group signatures. These are not elaborated here, but the interested reader can refer to the relevant literature.[16]

Apart from message identifiers, message contents may also be used to 'follow' a car. If the position of the car is indicated with great precision, a car can be tracked using only the contents of the messages it sends. A CAM or BSM message contains inter alia the 'Position', 'Heading', and 'Speed' of the car.[17] Receiving this information at moment t_0 would allow a receiver to calculate where the car will be in t_1 (say 1/10th of a second after t_0). At t_1 the car sends a new message conveying its current position. If that matches the position calculated on the basis of the data received at t_0 then both messages must originate from the same car.[18] Hence, the receiver could theoretically, and perhaps also practically, link all messages received from the same car together without using any message-identifier and thus be able follow a car through the contents of the messages received.

This problem is much less severe or even non-existent in an event-based system. In an event based system, messages are only sent if a car has 'noticed' a dangerous situation of which other motorists need to be warned. Because of the longer intervals between messages, it is much more difficult to calculate the position of a car at the end of the long interval solely based on the data received at the start of the interval. Hence, this is a strong privacy argument for preferring an event-based system over an awareness-based system.

However, in the future, self-driving cars likely need the more frequent information that only an awareness-based system can provide. Moreover, self-driving cars most probably need position information with a very high degree of

[15] For an overview, see Sapna S Kaushik, 'Review of Different Approaches for Privacy Scheme in VANETS' (2013) 5(2) *International Journal of Advances in Engineering & Technology* 356.

[16] Ibid.

[17] In fact, a CAM message also contains data like 'Path history', 'Drive direction', 'Longitudinal acceleration', 'Curvature', 'Yaw rate', 'Lane number', 'Steering wheel angle', and 'Lateral acceleration'.

[18] Krishna Sampigethaya et al, 'CARAVAN: Providing Location Privacy for VANET' (2005) <https://apps.dtic.mil/sti/pdfs/ADA459198.pdf>.

precision. Also, any possible solution based on selective use of the fields in a BSM message (for example, only communicate 'Position' and no other fields) may not be an option either.

2.4 Key Distribution

In the Car2Car consortium, a car will obtain a master certificate. This certificate is not used for communication. Rather, it is used to obtain pseudonym certificates that will be used for the actual communications between cars. In the Car2Car Consortium, each car has at least 20 pseudonym certificates active at the same time. The certificates are used for periods of at most a week. Every 10 to 30 minutes another certificate out of the set of at least 20 is used. Hence, if a car is used intensively, it may be that a certificate is reused a number of times within a week. Even though there may be some reuse of certificates, it is clear that each car needs many thousands of pseudonym certificates. It may not be possible to load a new car with enough certificates to last its entire useful life. Hence, at certain points, new key-pairs and certificates need to be distributed to the car.

2.5 Security

Road safety comes to depend on the correct functioning of On-Board-Units ('OBUs'). Through an unintentional defect or intentional manipulation, an OBU may start misbehaving, such as sending incorrect or misleading messages. In order to detect misbehaving OBUs, all OBUs have a capability to detect misbehaving OBUs in their vicinity, for example when the messages coming from a misbehaving OBU are inconsistent. OBUs that have detected the misbehaviour of another OBU no longer relies on messages originating from it. This is only a temporary solution, effective until the next pseudonym switch by the misbehaving OBU.[19] For a longer-term solution, a more centralised approach is needed, involving the Certificate Authority ('CA'). The CA may distribute a Certificate Revocation List ('CRL') containing all the pseudonyms attributed to the misbehaving OBU.[20] With many pseudonyms in circulation, CRLs may become very long lists. It may become difficult to check these lists in real-time. Perhaps, additional measures are needed to expel misbehaving OBUs, such as making the functioning of the OBU part of periodic technical check-ups of vehicles.

[19] David Antolino Rivas et al, 'Security on VANETs: Privacy, Misbehaving Nodes, False Information and Secure Data Aggregation' (2011) 34 *Journal of Network and Computer Applications* 1942, 1949–51.

[20] Mohammad Khodaei, Hongyu Jin and Panos Papadimitratos, 'Towards Deploying a Scalab' (2014) *IEEE Vehicular Networking Conference (VNC)* 33.

2.6 Confidentiality

Will messages be encrypted to maintain confidentiality? An important reason *not* to encrypt is latency. It may simply cost too much time to encrypt and decrypt messages. Another problem is that messages are broadcasted. Hence, you do not know who the receivers are. This in turn means that encryption would require that the key is shared among millions of cars — is a secret shared among millions still a secret? Obviously, the OBU will be a blackbox that does not allow a secret key to be read, just like that, but if many messages are sent using the same key, it is worthwhile for a hacker to try to crack the key. The risk that the key(s) is/are exposed is even bigger if a less robust encryption algorithm or a short key is chosen in the interest of limiting latency. Hence, from a purely technical perspective, encryption for confidentiality is a far from a self-evident choice.[21] However, without confidentiality, the identification risk is only countered by the short usage period of identifiers and the unobservability of identifier changes.

2.7 Conclusion about 'Code'

For technical protection of privacy, the automobile industry has chosen to allow unidentified participation in C-ITS. However, maintaining the unidentified status represents an enormous challenge in a system where one's vehicle broadcasts its position very regularly. Technology protects against identification, but it is stretched to its ultimate possibilities. Communications have to take place with near-zero latency. Pseudonym changes may be challenging to hide. Key distribution and Certificate Revocation are challenging. Encryption for confidentiality cannot be implemented in a way that makes technical sense.

3 *Privacy and Data Protection*

In the European Union, data protection is a fundamental right recognised in article 8 of the *European Convention on Human Rights*, and issues with data protection arising when the data is processed are dealt with according to the GDPR.[22] In the context of a safety warning system, the purpose of processing personal data is to warn a driver in case of a risk of a collision with another vehicle. In order to realise this system, location data must be shared with other vehicles. This data at least comprises of the location, speed, and heading of the vehicle. In an event-based system, the type of event must also be communicated (eg sudden braking). The messages within which these data are communicated

[21] No confidentiality in DSRC (US). George Corser, 'Threats in Vehicle-to-vehicle (V2V) Communication' (YouTube, 13 July 2014) 00:19:00 <https://www.youtube.com/watch?v=wArRijBW9uA >.

[22] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1.

contain technical identifiers such as the MAC-address and a public key certificate (which the Car2Car consortium calls 'pseudonym certificate'). They are used temporarily as described above.

3.1 Personal Data?

Before considering the protections for personal data under the GDPR, one must first determine whether the messages sent in the context of the safety warning system contain personal data. The messages contain public key certificates and MAC-addresses. Even though they are frequently changed in order to prevent identification, this does not necessarily mean that they qualify as anonymous according to the GDPR. Furthermore, the contents of the messages (the indication of place, speed, direction, and, in an event-based system, event) may be a profile that potentially qualifies as personal data.

Are the technical identifiers 'personal data' for the purposes of the GDPR? This question is relevant because it determines whether the GDPR applies. Article 4(1) GDPR defines personal data as follows:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

From this definition, it is clear that personal data need to relate to a natural person. The identifiers mentioned above relate to an OBU or to a vehicle, and not directly to a natural person. However, this does not necessarily disqualify these data as personal data. Information is related to a person, where it 'by reason of its content, purpose or effect, is linked to a particular person.'[23]

The messages sent out contain a public key (pseudonym) certificate and content, such as place, direction, and speed. As will be elaborated below, databases allow the pseudonym (ie the public key or MAC-address) to be linked to the owner and often also to the driver, since most owners drive themselves.[24] This gives

[23] *Nowak v Data Protection Commissioner* (Court of Justice of the European Union, C-434/16, ECLI:EU:C:2017:994, 20 December 2017) [35]. Cf Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology* (Working Paper No 105, 19 January 2005) 8. According to the Article 29 Working Party, 'data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.'

[24] The Dutch Statistical Office shows that in 2015, lease cars drove around 24 billion kilometres, whereas privately owned cars drove 91 billion kilometres: CBS, *Nederlanders en hun Auto* (Report, 2017) 11 <https://www.cbs.nl/nl-nl/achtergrond/2017/08/nederlanders-en-hun-auto>.

information about the driver, for example the places they visited. The owner and driver may also be affected, for example if speeding tickets were issued on the basis of message data.

Could message data still relate to our driver by way of purpose or effect, even if the data of a message (pseudonym and contents) do not resolve to the name of an owner or driver via a database? The contents of messages (place, speed, and direction) form a profile. Based on this profile, other vehicles do or do not display a warning to their drivers. Based on the warning or absence of a warning, other drivers make traffic decisions, for example to drive onto the road or to wait. Therefore, the data have an effect on the driver of our car, because they influence the decisions that other drivers make and thus affect our driver's safety. Indeed, the data are *intended* to have an effect on our driver, since it is a safety warning system. Furthermore, a system may lead to stigmatisation of certain groups, for example if it more often warns for young drivers than for older ones. Hence, the message data may very well be information 'relating to' our driver by way of purpose or effect,[25] even if the data do not resolve to a person identified by name and even though the (intended) effects may pertain to a limited domain. However, this does not mean that information about the underlying algorithm that decides how message contents leads to a safety warning qualifies as personal data, per the reasoning of the European Court of Justice in *YS, M & S*.[26]

The mere fact that, theoretically, message data can be related to natural persons is not enough to qualify them as personal data. It may simply be too difficult to find out to whom they relate. Recital 26 of the GDPR indicates the conditions under which a person is 'identifiable' in data:

> To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

From this recital and the definition of 'personal data', it is clear that the difficulty of identification depends on the means that are available to find out an identity, or more specifically, what means are reasonably likely to be used. Recital 26 of the GDPR further clarifies this aspect by stating:

[25] *Nowak v Data Protection Commissioner* (Court of Justice of the European Union, C-434/16, ECLI:EU:C:2017:994, 20 December 2017) [35]. Cf Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology* (Working Paper No 105, 19 January 2005) 8. According to the Article 29 Working Party, 'data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.'

[26] *YS, M and S v Minister voor Immigratie, Integratie en Asiel* (Court of Justice of the European Union, Joined Cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081, 17 July 2014).

> To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

Is a participant identifiable for the controller(s), assuming for the purposes of analysis here that the controllers are the manufacturer of the vehicle and drivers of other vehicles? Where the controller can reasonably call in the help of another person, the capabilities of this other person are taken into account as well.[27] There may be exceptional circumstances (as elaborated below) in which a controller can call in the help of possessors of relevant databases. Usually, a driver will not have access to databases that allow the identification of other drivers or owners from the pseudonyms that their vehicles use to send messages. However, it is conceivable that in certain circumstances, drivers can retrieve identities from databases with the help of authorities. A likely context would be identification of hit-and-run drivers, ie drivers who flee the site of an accident without making their identity known. The messages sent by the hit-and-run vehicle may have been received by the vehicle that stayed behind at the scene of the accident.[28] With the aid of databases, the identity of the runaway driver may be retrieved from the pseudonyms their vehicle used to send messages. This would make the pseudonyms 'personal data' for the drivers of other vehicles.

This interpretation accords with a view expressed by the Article 29 Working Party in an analogous situation concerning clinical trials (where a pharmaceutical company only holds a key and a researcher only holds the mapping from the name of a test-person to the key. If a test-person needs medical treatment, it is necessary to retrieve what test medicines have been administered to him):[29]

> The pharmaceutical company has construed the means for the processing, included the organisational measures and its relations with the researcher who holds the key in such a way that the identification of individuals is not only something that may happen, but rather as something that must happen under certain circumstances. The identification of patients is thus embedded in the purposes and the means of the processing. In this case, one can conclude that such key-coded data constitutes information relating to identifiable natural persons for all parties that might be involved in the possible identification and should be subject to the rules of data protection legislation.

[27] *Patrick Breyer v Bundesrepublik Deutschland* (Court of Justice of the European Union, C‑582/14, ECLI:EU:C:2016:779, 19 October 2016).

[28] For accident analysis purposes, messages need to be retained for less than a minute. Only when an accident happens will data be kept: *Digital Rights Ireland* (C-293/12) [2013] ECR I-845; *Tele2* (C-203/15; C-698/15) [2016] ECR I-970. Cf *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'* (Court of Justice of the European Union, C-13/16, ECLI:EU:C:2017:336, 4 May 2017) [34].

[29] Article 29 Working Party, *Opinion 4/2007 on the Concept of Personal Data* (Working Paper 136, 20 June 2007) 19–20.

In conclusion, pseudonyms are 'personal data' for a driver whose vehicle receives messages containing those pseudonyms.

A manufacturer may assume a network maintenance role that would involve the removal of misbehaving OBUs. As described above, individual OBUs can detect misbehaving nodes. These detections need to be reported to a central actor, assuming for our purposes here that this central actor is the manufacturer. The manufacturer would then evaluate the reports received from OBUs and decide which OBUs need to be withdrawn from service. With the help of the Certificate Authority ('CA') and/or a Registration Authority ('RA'), all pseudonyms used by the OBU may be identified and placed on a CRL. As we saw above, CRLs may not function well in the context of C-ITS because of their length and the need to evaluate them real-time. Therefore, additional measures to remove misbehaving OBUs may be needed. The databases of the RA/CA may also yield a serial number of the OBU or the vehicle, through which the owner or driver may be identified. This identification would allow additional measures to be taken, such as directly addressing the owner or driver of the vehicle or causing the vehicle to fail its periodic technical check-up.

A possible argument against the qualification of messages as personal data is the transient nature of the data received by a vehicle. The data merely serves to generate a safety warning for the driver. The OBU does not display the message or its contents (only a warning) and it is discarded when no longer needed for warning the driver or reconstructing an accident. So, after a minute, a received message is deleted. In literature, it has been argued that transient data should not be considered personal data, especially if the data is not accessible for its controller and therefore the controller cannot identify a data subject.[30] However, even though the safety warning system uses the data only transiently, it is questionable that the data in messages are not personal data. The warning system is not closed and the data can be received unencrypted by anybody. With the data accessible by anybody, it is obviously also accessible by the controller. The lack of confidentiality is a risk that does not allow for the data to be kept outside the protective scope of the GDPR.

In conclusion, the GDPR is applicable to the safety warning system for both manufacturer and driver.

3.2 Grounds for processing

A vehicle participating in the warning system sends and receives messages. The sent messages contain personal data of the sending vehicle's driver or owner. The received messages contain personal data about the driver or owner of another vehicle. The receiving driver is potentially controller of the data received from

[30] Damian George, Kento Reutimann and Aurelia Tamò-Larrieux, 'GDPR Bypass by Design? Transient Processing of Data Under the GDPR' (2019) 9(4) *International Data Privacy Law* 285, 294–5.

the other vehicle; the other vehicle's driver is the data subject. Sometimes the data that vehicle B receives from vehicle A is passed on to vehicle C (for example when warning for the tail of a traffic jam). Then driver B sends a message containing both data pertaining to himself and pertaining to driver A, which makes B as sender also a controller.

This part of the article examines the bases for lawfully processing the received data by visiting the six grounds contained in article 6(1) of the GDPR. The article will first address the grounds in subclause (d) about vital interest of the data subject and (f) about legitimate interests of the controller. These grounds seek to find a balance between benefits and risks, though they do so in different ways. Then, the article will deal with the grounds in subclause (a) and (b) regarding consent and performing contracts, respectively. These grounds seek lawfulness in the exercise of autonomy by the data subject. Finally, the article will address the grounds in subclause (c) and (e) on legal obligation and public interest. These grounds find lawfulness in legality.

3.2.1 Vital Interests

According to recital 46 of the GDPR:

> The processing of personal data should be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis.

A vital interest appears to be usable as a ground for processing data only where the life of the data subject, or possibly somebody else, is at risk. This readily excludes awareness-based systems which broadcasts personal data irrespective of whether any danger is present. In an event-based system, messages are only sent where there is an event that other drivers need to be warned of. Envisioned Day-1 applications include hazardous location notifications, such as warnings for slow or stationary vehicle(s) and traffic ahead, road works, weather conditions, emergency braking, and an approaching emergency vehicle. These are the most dangerous applications, and will be supplemented with less dangerous events. It is questionable that the situations warned for are sufficiently severe threats to the life of a person so as to justify the 'vital interest' ground for lawful processing.[31] These are circumstances that motorists encounter daily and that give rise to accidents only in a very small fraction of the cases. However, the processing of personal data takes place even where the risk is very small and does not materialise. Therefore, the vital interest ground appears not to be usable as a basis to render the processing of personal data in these safety warning systems lawful.

[31] Data Protection and Privacy Working Group of the Cooperative Intelligent Transport Systems ('C-ITS'), *Processing Personal Data in the Context of C-ITS* (Submission to Article 29 Data Protection Working Party, 1 March 2017) 27.

3.2.2 Legitimate Interests

Article 6(1)(f) requires that, to be lawful:

> Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

According to the Article 29 Data Protection Working Party, this is not a subsidiary ground to be applied solely when no other grounds apply.[32] We will look at the (legitimate) interest of the controller first, then at the impact on the data subject, and finally at the balance to be struck.

In the C-ITS context, the basic interest of any controller is to prevent road accidents. If the driver is the controller, this is evidently a self-interest of the controller. Meanwhile, the manufacturer has a commercial interest — a safer vehicle is arguably more attractive for customers and easier to sell. There is also a clear societal interest in reducing the number of road accidents and lessening the adverse consequences of road accidents. This societal interest finds recognition with the EU, which actively encourages the development of the safety warning system. In April 2016, the EU published a roadmap for the development of C-ITS that foresees a Day-1 application of the safety warning system as a concrete output.[33] In the context of the protection of the right to health, the *European Social Charter* obliges its members either directly or in cooperation with public or private organisations to take appropriate measures to prevent accidents.[34] The interest appears to be legitimate: it is lawful, sufficiently specific, and it is actually pursued.

The safety warning system requires that data about the location of vehicles is shared, which as we saw above is information relating to natural persons. Without information about vehicles that are in the vicinity, giving motorists safety warnings is not possible. The system is set up in such a way that the bare minimum of data is shared.[35]

[32] Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (Working Paper No 217, 9 April 2014) 9.

[33] European Commission, *MOVE.DDG1.C.3, A Master Plan for the Deployment of Interoperable Cooperative Intelligent Transport Systems in the EU* (Roadmap Document, 7 April 2016).

[34] *European Social Charter (Revised)*, opened for signature 3 May 1996, ETS 163 (entered into force 1 July 1999) art 11(3) ('*ESC*'). This provision does not have an analogue in the *Charter of Fundamental Rights of the European Union*. However, all EU member States are party to the *ESC*.

[35] Cf *TK v Asociația de Proprietari bloc M5A-ScaraA* (Court of Justice of the European Union C-708/18, ECLI:EU:C:2019:1064, 11 December 2019) [46]–[51].

Sharing location information has a potentially significant impact on the data subject. Information about where the data subject has been in the past gives a telling insight into their life. Moreover, in the context of the warning system, location data are generated with high frequency and high precision. The risk of data 'leaking' from the warning system is not completely imaginary. The DENM and CAM messages are broadcast without encryption.[36] They are regularly received by other cars encountered on the road and by roadside units. The protection against identification merely rests on pseudonymisation. The risk that data are compromised is relevant under this ground for processing. For example, the prospect of a compromise may decrease the acceptance of the system and an actual occurrence of a compromise can cause distress to those involved.[37] At the same time, a data subject participating in the warning system expects to remain unidentified.

In conclusion, a safety warning system is in the wider community interest. At the same time, the data subject incurs substantial risks, given that location data are sensitive;[38] the data comes into the 'hands' of many parties that are not subject to effective governance at present; and the data are broadcast without encryption. The balance is not plainly in favour of the legitimate interests of controller. Hence, it needs to be examined whether additional safeguards can tip the balance in favour of making the processing lawful on this basis.

Giving the data subject/driver the possibility to opt out may help.[39] A driver who values highly the confidentiality of their location data would then have a realistic option of not sharing their data. However, it is difficult to make opting out work in practice. Taking account of the fact that a vehicle can be used by more than one driver, the option to opt out would need to be presented every time the engine is started. A driver not wishing to share their location data therefore would have to opt out every time they use the car. This quickly becomes a nuisance, with the risk that the default becomes the norm not because the driver chooses so, but because the acts required to opt out are too burdensome.

Admittedly, the problem of repetitive opt-out may be resolved with technology: it is possible to recognise a repeat driver, for example with biometrics. However, this raises new issues. Even more data about a driver would need to be stored,

[36] 'Leaking' in the context of the safety warning system is perhaps a somewhat misleading term, because it may suggest that ordinarily confidentiality is secured, which is not the case.

[37] Article 29 Data Protection Working Party, *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC* (Working Paper No 217, 9 April 2014) 37.

[38] Ibid 38.

[39] Article 29 Data Protection Working Party, *Opinion 03/2017 on Processing Personal Data in the Context of C-ITS* (Working Paper No 252, 4 October 2017) 10.

links between journeys can theoretically be made, and biometrics technically do not function adequately under all circumstances.

In conclusion, in this context, an opt-out system does not give a real choice *not* to participate. Perhaps this can be redressed via an opt-in system instead. However, opt-in raises the question of whether the legitimate interest of the controller is the ground on which the data processing is based. Rather than justifying the data processing by reference to a balance between the interests of the controller and the data subject, an opt-in system finds justification in the data subject's autonomy.

3.2.3 Consent

Article 6(1)(1) provides that processing will be lawful if 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes'. Any consent needs to be informed and freely given. In order to assess whether a valid consent to processing personal data in the safety warning system context can be given, it needs to be established how the consent is solicited and obtained. It is clear that a consent cannot be solicited real-time, ie when a vehicle encounters another vehicle on the road and they start exchanging messages. The only practical way is that the driver gives consent when they start the engine of the car. So, it stands to reason that the manufacturer makes sure that the vehicle solicits consent at that point. The controller who relies on the consent will often be a driver of another vehicle or its manufacturer.[40] Hence, the consent must be communicated from the place where it is solicited to the controller who relies on it. A practical way to address this would be to add a consent field in messages indicating whether consent has been obtained and perhaps giving detailed information about the modalities of the consent. Currently, the message content standards do not have a field that caters for this need.

Having established that the manufacturer solicits consent, the next question is how the manufacturer can do so. A valid consent cannot be obtained by switching the safety warning on by default and giving the driver the possibility to opt out.[41] The driver must be asked to perform some act to consent to their data being shared within the safety warning system. From a practical perspective, this makes it hard to rely on consent, because the attention of the driver must be directed to the safety warning system before they start driving.

[40] Each driver can only be considered controller in respect of the data they process and only need to obtain consent for these processes. Cf *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (Court of Justice of the European Union C-40/17, ECLI:EU:C:2019:629, 29 July 2019) [101]. However, this does not mean that a controller cannot make use of the services of others to solicit and obtain consent.

[41] *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* (Court of Justice of the European Union C-673/17, ECLI:EU:C:2019:801, 1 October 2019) [55].

An interesting question is whether consent needs to be solicited repeatedly. A car can be used by more than one driver. Therefore it can be questioned whether a consent obtained before a ride today can be relied on tomorrow for another ride in the same vehicle. If consent is solicited before each ride, a concern is that data subjects simply give consent by clicking without knowing what they consent to. [42] Consent becomes more an excuse for processing instead of a well-considered permission. This concern is particularly pertinent with respect to the safety warning system because of the special risks that the horizontal peer-to-peer architecture poses to data protection.

Informed Consent

Consent needs to be informed in order to be valid. As was discussed above, in practical terms, the task of informing the driver will fall on the manufacturer of the vehicle, who is also the party soliciting the consent. A question is whether the manufacturer can inform the driver adequately about the implications of a consent. The safety warning system is not closed and data are broadcasted without encryption that could otherwise protect confidentiality. Anybody may receive and read the data and process them. Hence, it may be impossible to inform the driver of what will happen to their data.

Theoretically, there are ways to escape the conclusion that informed consent is impossible. First, the system may be changed and messages may be encrypted. However, this would be rather pointless as we have seen above. The key to unencrypt messages would need to be shared amongst millions. A system with encryption would be compromised in effectiveness (slower and less safe because of encryption) without actually solving the issue. Secondly, the data in a message may be qualified as anonymous for third parties and not just as pseudonymous. The analysis in section 3.1 focused on the question of whether the data were anonymous for the regular controllers (which they were not). This does not preclude the possibility that the data may be anonymous for third parties.

The discussion then requires examining whether third parties can identify a natural person from the data. In this analysis, one must take into account all means that a third party reasonably likely uses for identification.[43] Since these means are brought to the table by an unknown third party, it is unclear what 'reasonably likely' entails here. You can go at least two ways. On the one hand,

[42] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (May 25, 2016) <http://dx.doi.org/10.2139/ssrn.2784123>. This academic report suggests that consent is so often *not* informed, that reform should consider abolishing it as an independent ground for processing of personal data.

[43] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regards to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC* (General Data Protection Regulation) [2016] OJ L 119/1, recital 26 ('*GDPR*').

you may say that the criterion points away from an absolutist stance by emphasising the reasonableness aspect. As a criterion figure for the third party, you may choose a rational hacker who will not spent more resources on identification than the benefits they expect to obtain. On the other hand, you may argue that the data are spilled into the public domain for anybody to pick up. In other words, the number of potential hackers is so large that you must also consider the brilliant but irrational hacker. In other words, you emphasise the term 'likely', which you interpret as 'given enough eye-balls, all bugs are shallow'. Or put differently: in the fullness of time, a hard-nosed hacker will rise and a system is as weak as the most hard-nosed hacker is capable. I incline towards the stance that the system needs to be seriously discouraging for a rational hacker, but I must admit that it is an open issue.[44] This places a big question mark over consent as a basis for processing location data in the context of C-ITS.

Freely given consent

Consent also needs to be given freely. A warning system may be set up in such a way that a driver can choose to switch on the OBU and participate fully, or alternatively leave the OBU switched off and not participate at all. This implies that a driver refusing consent cannot benefit from the safety warning system. Since safety is a basic need, withholding safety can exert an undue pressure on a data subject to consent. In these circumstances, consent would not be freely given.

However, the system can be set up in an alternative way so that a driver can choose not to send data, while still being able to receive data. The driver would free-ride the system, or to formulate more positively, they protect their own privacy by not sending data about themselves, but can still benefit from safety warnings. This takes away the pressure to consent. Moreover, research by Schindhelm and others shows that the benefits of a V2V safety system equal or

[44] Michael Kiometzis, 'Privacy Considerations for C-ITS and the Connected Vehicle', *Federal Commissioner for Data Protection and Freedom of Information* (BfDI) <https://docbox.etsi.org/workshop/2018/20180306_ITS_WORKSHOP/S02_CITS_NEXT_CHALLENGES/PRIVACY_CITS_CONNEC_VECH_BFDI_KIOMETZIS.pdf>. Kiometzis argues that anonymisation is not possible given the many technical ways to track. Wouter van Haaften and Tom van Engers, 'Data Protection and C-ITS — Personal Data' (Conference Paper, 12th ITS European Congress, 19–22 June 2017) <https://pure.uva.nl/ws/files/29069847/20170423_DataprotectionandC_ITS_vanhaaften_vanengers.pdf>. They argue that C-ITS can be set up to work without personal data. They base their view on Case C-582/14, judgment 19 October 2016. The means for identification are, according to them, not reasonably likely available to members of the public.

surpass the costs at penetration rates as low as 6.1 to 8.7 percent.[45] A system that allows free-riding therefore needs not be excluded on safety reasons.

That said, the utility (safety gains) that the system could offer diminishes if the number of drivers contributing their data to the system drops as a consequence of offering the possibility to free-ride the system. Hence, choosing consent as the ground for processing involves a trade-off.

In conclusion, it is important to respect the autonomy of the driver and owner to decide whether to share their personal data. However, it is questionable whether consent is the way to realise that. In practical terms, it is hard to solicit consent in a way that the data subject makes a well-considered decision about data sharing. Moreover, it is doubtful that the data subject can make an informed decision given the lack of closure of the system (even if you consider that the chance of non-participants listening in is small). Finally, consent as the basis for processing data may act as a disincentive to share data, and diminish the utility of the safety warning system.

3.2.4 The Performance of a Contract

The second ground the GDPR offers for processing is necessity for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract. Such contract has to be a contract to which the data subject is party. In the C-ITS context, the driver is the data subject, but it is not a given that the driver is party to a contract. Situations where a contract with the data subject is lacking, may be where a C-ITS subscription is concluded with an owner/non-driver such as a lease company or the employer of the driver.

Not only are data subjects not necessarily party to a contract, the fact that a car may have different drivers complicates the use of contract as a ground for processing personal data. The driver needs to accede to an existing contract or needs to conclude a mobile-commerce contract with the provider of the warning system. Acceding to or concluding a contract likely requires a positive act by the driver, signalling acceptance of an offer to enter into a contract.[46] In the absence of a positive act (eg 'by driving this car, you accept …'), acceptance by the driver and the existence of a contract is most uncertain, since it is unclear that driving the car can be interpreted as acceptance. For practical purposes, this basis is too shaky. Hence, a positive act signalling acceptance is needed.

[45] Roland Schindhelm et al, 'Socio-Economic Viability of SAFESPOT Cooperative Safety Systems' (Conference Paper, European Conference on Human Centred Design for Intelligent Transport Systems, 29–30 April 2010).

[46] Frederik J Zuiderveen Borgesius, 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) 5 (3) *International Data Privacy Law* 163, 165–6.

If multiple drivers share a car, a problem arises regarding how to know whether the present driver has accepted the contract in the past. Asking the driver to confirm acceptance every time the engine is started is not very user-friendly and will quickly be felt as a nuisance. However, requiring the driver to perform a positive act to signal acceptance is not so burdensome if the driver would need to do this only once. Recognising a repeat driver with biometric means could achieve this, but would bring about new privacy concerns. Perhaps if a car becomes a mobile-commerce platform in the future, logging in to the car (through biometrics or otherwise) may become a normal procedure that serves many purposes. However, for the near future, this is a step too far.

In any case, the data processing needs to be necessary for the performance of the contract. The difficulty here is less so about finding out what processing of data is necessary, but rather to make sure that the various controllers and processors of data, such as other drivers, manufacturers and road managers actually limit their processing to what is needed for performance of the contract. An adequate governance structure needs to be in place to ensure that data processing is both limited to what is needed and only done by those who are supposed to do the processing. That is a challenge given that such structure would need to cover multiple manufacturers, drivers, and road managers.

In conclusion, contract as a ground for processing is difficult to realise, since the driver as a data subject needs to be a party to the contract and it is challenging to ensure that processing stays within the boundaries of what is necessary for the performance of the contract.

3.2.5 A Legal Obligation to which the Controller is Subject

Article 6(1)(c) provides that processing is lawful if it 'is necessary for compliance with a legal obligation to which the controller is subject'. Currently, there is no legal obligation for vehicle manufacturers to install a safety warning system as discussed here and to process the relevant data.[47] The creation of a legal obligation to process location data requires justification. Such justification needs to address both the benefits of the data processing and risks to the data subject.

[47] *Commission Delegated Regulation (EU) …/... Of 13.3.2019 Supplementing Directive 2010/40/EU of the European Parliament and of the Council with Regard to the Deployment and Operational Use of Cooperative Intelligent Transport Systems* [2019] C(2019) 1789 final, recital 23: 'Such processing should have an appropriate legal basis, as listed in Article 6 of Regulation (EU) 2016/679, which is not provided for by this Delegated Regulation.' The European Commission did not mention mandatory V2V communication in its Communication about a European Strategy on C-ITS. See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy on Cooperative Intelligent Transport Systems, a Milestone Towards Cooperative, Connected and Automated Mobility' (COM(2016) 766 final, 30 November 2016).

On the benefits side, a development towards more self-driving vehicles is anticipated. In addition to their on-board sensors, self-driving vehicles will increasingly rely on communication with other vehicles and infrastructure. Broad participation in location communication becomes more important and it is likely that vehicles, at some point, will be mandatorily equipped with the technology to communicate their position and heading.[48] In the US, developments are going in the same direction. The US National Highway Traffic Safety Administration released a notice of proposed rulemaking mandating V2V communication in all new vehicles and trucks sold.[49]

On the risks side, the data processing risks for the data subject do not disappear. Nonetheless, a legal obligation offers opportunities to improve the protection of data subjects as well. The general binding character of a legal obligation can be put to use. The peer-to-peer character of C-ITS makes it difficult to set up a governance structure with sufficient grip on the various controllers and processors of personal data, absent a legal instrument directly binding them. Introducing an EU-wide legal obligation would give the processing of data a legal basis and an opportunity to specify adequate protection for data subjects.[50] It also makes opt-in or opt-out options, as well as any biometrics needed to make opt-in or opt-out practically possible, superfluous.

Given these considerations, it makes sense that a legal obligation to process the personal location data in the C-ITS context will be created at some point.

3.2.6 Public Interest

The final ground discussed here is public interest under article 6(1)(e). This ground makes processing lawful if it 'is necessary for the performance of a task

[48] See also C-ITS Platform, *Final Report Phase II* (Report, September 2017) 28; Joost Vantomme, 'Cooperative, Connected and Automated Mobility. Quo Vadis? Challenges for the Automotive Industry' (Conference Paper, PZPM Conference, 26 February 2018) 5 <https://www.pzpm.org.pl/pl/content/download/8262/45904/file/20180226%20CCAM%20challenges%20ACEA%20presentation%20PZPM%20Warsaw_.pdf>.

[49] National Highway Traffic Safety Administration, Department of Transportation, *Federal Motor Vehicle Safety Standards; V2V Communications*, 49 CFR Part 571 [Docket No NHTSA-2016-0126] RIN 2127-AL55. See also Christopher H Grigorian and R Nicholas Englund, 'United States: NHTSA And Motor Vehicle Safety', *Mondaq* (online, 23 January 2019) <http://www.mondaq.com/unitedstates/x/775678/cycling+rail+road/NHTSA+And+Motor+Vehicle+Safety> stating that the proposed rulemaking is still in flux.

[50] C-ITS Platform, *Final Report Phase II* (Report, September 2017) 28. Article 29 Data Protection Working Party, *Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS)* (Working Paper No 252, 4 October 2017) 9.

carried out in the public interest or in the exercise of official authority vested in the controller'.

According to article 6(3) of the GDPR, this ground requires a legal basis. This legal basis concerns the public-interest task, not specifically the processing of data. The processing of the data must however be necessary for fulfilling the task. *Directive 2010/40/EU* on the Intelligent Transport Systems framework states that this framework addresses 'increasing congestion of road infrastructure and rising energy consumption, as well as … environmental and social problems'.[51] There is a public interest to address these issues. However, the directive does not vest in particular actors the task to bring about Intelligent Transport Systems.

At present, the legal basis for applying the ground of article 6(1)(e) is doubtful. Given that there is a certain public interest in C-ITS, a legal basis could be created. It would need to be clear how governance of C-ITS will be set-up, so that the task can be vested in actor(s) that are in a position to realise meaningful protection for data subjects.

4 Conclusion

The safety warning system that the EU seeks to establish is believed to make a substantial contribution to road safety. However, from a data protection perspective, there are undeniable risks. The location data broadcast by a vehicle are personal data about the driver/owner of the vehicle. They are communicated without confidentiality to an unlimited group of potential receivers. Currently, the protection of the data subject predominantly rests on pseudonymisation. When assessing the adequacy of grounds for lawful processing of personal data, it appears that a balance between benefits and privacy risks as required by subclause (f) (legitimate interest of the controller) is not evidently present. Hence, it is worthwhile to assess whether giving the driver the choice to share their data could bring the system within the ambit of a lawful processing ground.

A driver can indicate their choice and the modalities of their choice via opt-out (legitimate interest) or opt-in (consent, performance of contract) systems. However, working with declarations by the driver in a horizontal peer-to-peer system meets various complications. Since vehicles can be used by multiple drivers, there is a need to recognise repeat drivers in order to not bother the driver every time the engine is started, but recognising repeat drivers (eg through biometrics) carries its own risks. Building on driver declarations is also difficult for the controllers who rely on the declarations. The messages sent would need to be adapted to incorporate fields in which the modalities of the choice are indicated. Finally, it is also difficult to ensure that the various controllers

[51] *Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the Framework for the Deployment of Intelligent Transport Systems in the Field of Road Transport and for Interfaces with Other Modes of Transport* [2010] OJ L 207/1, recital 1.

implement the indicated choices, given the horizontal character of the system and the multitude of controllers. These complications are not insurmountable but may take a long time to realise because they require coordination between a large number of stakeholders.

The need for and the interest of position communication will only grow since cars get ever more self-driving capabilities. With stronger reliance on inter-vehicular location communication, broader participation becomes more important. Self-driving cars in all likelihood will heavily rely on communication with other traffic participants. It is not unlikely that the safety of self-driving vehicles requires a legal duty to participate in location sharing. Therewith, the case for a legal obligation as the formal ground for processing (under subclause (c)) will become stronger over time. A legal obligation offers the opportunity to specify the responsibilities of the various controllers, so that the risk of lack of clarity about the existence and contents of responsibilities is minimised. Lower legislation can lay down further requirements that location communication must meet in order to maintain an acceptable level of data protection. For the legislator, it is not unwise to get in lane for that future development now.